w odniesieniu do całych dokumentów, a jedynie do ich skrótów, bo tak jest szybciej (ta technika nosi nazwę „hash then sign"). Przez to podpis może być wykorzystany przez fałszerza dokumentu wbrew intencjom podpisującego. Więcej na ten temat można poczytać na stronie [1], gdzie znaleźć można także przykład takiego fałszerstwa: dwa różne pliki PS o tym samym skrócie MD5.

Algorytm SHA-1 pozostaje póki co bezpieczny, choć powstały techniki ataku wymagające znacznie mniej niż 2^{80} testów. Próby takie są podejmowane, ale kolizje znaleziono na razie jedynie dla uproszczonych wersji tego algorytmu. Istnieje także nowszy standard, SHA-2, którego różne wersje generują klucze 224, 256, 384 i 512-bitowe. Stopień skomplikowania tego algorytmu jest jeszcze większy niż w przypadku MD5 i SHA-1; występują w nim także różne dziwne stałe, na przykład części ułamkowe liczb postaci $\sqrt[3]{p}$, gdzie p jest liczbą pierwszą. W związku z zagrożeniami atakami National Institute of Standards and Technology (NIST, amerykańska jednostka rządowa zajmująca się między innymi standaryzacją) zaleca całkowitą rezygnację z MD5 na rzecz SHA-1, a po roku 2010 rezygnację z SHA-1 na rzecz wariantów SHA-2. Nie będzie to takie proste, bo SHA-1 jest dziś częścią powszechnie używanego standardu podpisów cyfrowych Digital Signature Algorithm.

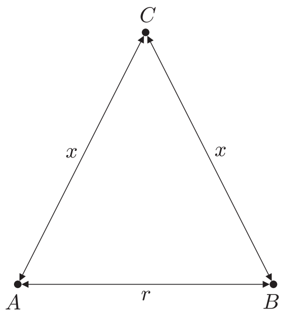
Niedawno (w listopadzie 2007) NIST ogłosił konkurs na nową funkcję skrótu, która zastąpi MD5 i warianty SHA. Będzie ona nosiła nazwę SHA-3. Kandydatury można zgłaszać do 31 października 2008 roku, po czym, po czterech latach przeznaczonych na kolejne rundy publicznej dyskusji, nowy standard ma zostać wybrany i ogłoszony w 2012 roku. Projekty muszą zawierać dokładną specyfikację wraz z implementacją oraz uzasadnienie takiej a nie innej konstrukcji algorytmu, doboru parametrów i stałych oraz, w miarę możliwości, analizę odporności na różne rodzaje ataków. Nowa funkcja musi być zdolna do generowania skrótów o długościach 224, 256, 384 i 512 bitów. Podstawowymi kryteriami decydującymi o wyborze zwycięzcy będą: bezpieczeństwo, koszt czasowy i pamięciowy obliczania funkcji oraz dodatkowe cechy algorytmu, takie jak np. łatwość zrównoleglania.

[1] `http://www.cits.rub.de/` `/MD5Collisions/`
[2] `http://www.nist.gov/hash-competition`
[3] `http://en.wikipedia.org/wiki/` `/{MD5,SHA}`

Zadania

Redaguje Ewa CZUCHRY

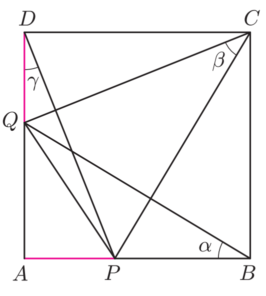
F 715. Dwie gwiazdy okrążają wspólny środek masy ze stałymi co do wartości prędkościami liniowymi v_1 i v_2 oraz T. Znaleźć masy gwiazd oraz odległość między nimi,
Rozwiązanie na str. 8



F 716. Dwie gwiazdy A i B o masie M każda, znajdujące się w stałej odległości r, pod działaniem wzajemnego przyciągania grawitacyjnego poruszają się po orbitach kołowych (rysunek). W pewnej nieznanej odległości od gwiazd, w tej samej płaszczyźnie, znajduje się lekka planeta C. Znaleźć tę odległość, wiedząc, że $AC = BC = x$, oraz że rozmiary trójkąta ABC nie zmieniają się w czasie ruchu układu.
Rozwiązanie na str. 9

Redaguje Waldemar POMPE

M 1204. Każdy punkt okręgu pomalowano na jeden z dwóch kolorów. Wykazać, że istnieje trójkąt równoramienny wpisany w ten okrąg, którego wszystkie wierzchołki mają ten sam kolor.
Rozwiązanie na str. 10



M 1205. Punkty P i Q leżą odpowiednio na bokach AB i AD kwadratu $ABCD$, przy czym $AP = DQ$ (rys.). Obliczyć

$$\sphericalangle PBQ + \sphericalangle PCQ + \sphericalangle PDQ\,.$$

Rozwiązanie na str. 11

M 1206. Rozstrzygnąć, czy istnieje takich 100 liczb naturalnych $a_1, a_2, \ldots, a_{100}$, że dla $i \neq j$ liczba a_i^2 jest podzielna przez a_j, a liczba a_i nie jest podzielna przez a_j.
Rozwiązanie na str. 15